Brute-force, Dictionary Attacks and Mitigation

JOÃO BETTENCOURT

Fakulteta za elektrotehniko, računalništvo in informatiko, Univerza v Mariboru
Email: joao.bettencourt@um.si

The increasinng volume on digital systems in the modern society has increased the importance of security measures. One of the most persistent threats to digital security is the brute-force and dictionary attack, which exploits weak passwords to be harmful to systems. This paper explores these attack techniques, their mechanisms, and their impact on the modern society. By understanding the key points behind brute-force and dictionary attacks, we can identify vulnerabilities in password systems and propose effective mitigation strategies. This topic was chosen due to its significant relevance in today's digital age, where establishing security standards and practices is essential for protecting sensitive information. The study also emphasizes the need for stronger authentication methods and awareness to protect against evolving attack techniques. By combining theoretical analysis with practical demonstrations using tools such as Kali Linux, this work aims to highlight not only the risks posed by these attacks but also measures to improve digital security.

Keywords: Brute-Force Attacks, Dictionary Attacks, Password Security, Cybersecurity.

1. INTRODUCTION

Password-based authentication remains one of the most common methods for system security, based on their simplicity and effiency. However, it continues to show significant vulnerabilities, facing brute-force and dictionary attacks. Those methods exploit the inherent weaknesses of user-created passwords, which are often short, predictable and based on common patterns. In spite of decades of research and development of numerous countermeasures, the human factor remains the weakest link in the security trifecta.

By the new advancements in computational power, these vulnerabilities got aggravated, making attackers more effient cracking passwords. A task that used to require days now takes seconds or even less. At the same time, passwords cracking techniques have become progressively sophisticated, including vast dictionaries, permutations, and adaptive algorithms. These developments highlight the critical need for powerfull mitigation strategies that not only address technical vulnerabilities but also focus on improving user practices

This study investigates the mechanics of brute-force and dictionary attacks, demonstrates their effectiveness using practical experiments, and evaluates their strengths and weaknesses of most commonly used mitigation strategies. By analyzing passwords, by their entropy and characteristics, this work aims to emphasize the importance of adopting strategies to mitigate these attacks, by adopting stronger password

policies and multi-factor authentication methods.

2. EXECUTION OF THE ATTACKS

Attacks...

2.1. Regular Expressions

Regular Expressions and What was used in this project

2.2. Brute-force Approach

How the Brute-force Approach happened

2.3. Dictionary attack Approach

How the Dictionary Approach happened

3. ANALYSIS

Analysis of what was done before

4. MITIGATION STRATEGIES

Short description of what is a mitigation strategie

4.1. Account Lockouts

After X number of attempts locks and account

4.2. Captcha

Side bard captcha to prevent software to imitate human behavior, such as bots or botnets

4.3.   Multi-factor Authentication

such as an additional password, token, smartphone or
biometric data

4.4.   Password lenght

password lenght from 15-25

4.5.   SALT

adding salt to when a password is hashed in the
database

5.   CONCLUSION

6.   REFERENCES